US Critical Infrastructure Faces Cyberwarfare-- Every Day.

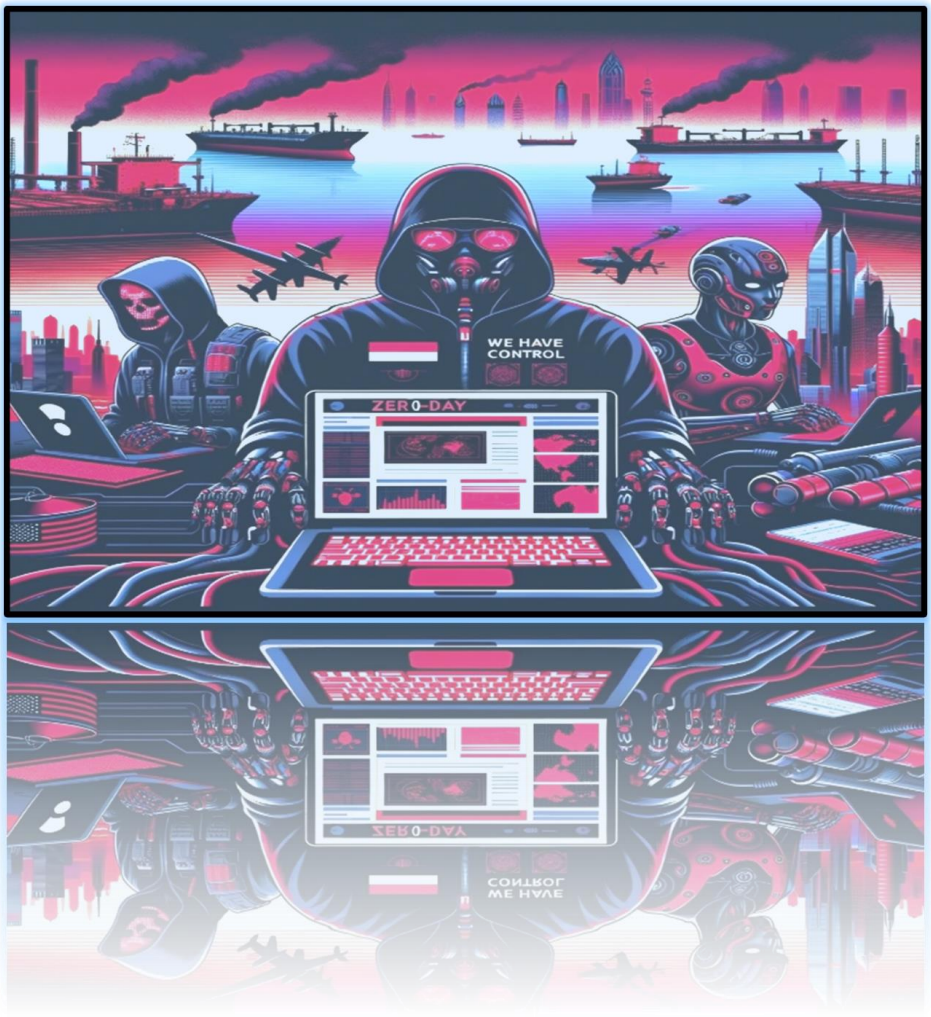


ILLUSTRATION : Fred Ellison: GENERATED BY: DALL-E (OpenAI)

DALL·E is an AI program developed by OpenAI that specializes in generating images from textual descriptions. It uses a version of the GPT (Generative Pre-trained Transformer) architecture, which is known for its ability to understand and generate human-like text and extends this capability to the realm of visual creation.””

NORTHERN CALIFORNIA

AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
December 2023 (Edition 2023-12)

TABLE OF CONTENTS

Dear Readers,

I would like to take a moment to thank each one of the members of the AMSC Cyber Sub-Committee for participation during 2023. Additionally, a special thank you to Paul Martin, LT. Chris Payne, LCDR Oviatt and CDR Pohl, for "taking the time." Many thanks to those who have invested time in making my first year grand. My first 2024 goal--to host a live in person meeting.

Finally, I have studied Sun Tzu, "The Art of War," for many years, and begin this report by offering you the quote I've shared with fellow Army soldiers, friends, colleagues, the many kids I've coached in sports as well as my own kids. I live it every day.

Sun Tzu said: Whoever is first in the field and awaits the coming of the enemy, will be fresh for the fight; whoever is second in the field and has to hasten to battle will arrive exhausted.

Thank you,

Fred Ellison

EXCUTIVE SUMMARY

This year-end report offers a unique examination of the evolving cybersecurity landscape within **critical infrastructure** with a focus on the **maritime sector**. We highlight the **confluence and sophistication of nation state actors and the uncomfortable Truths about the US** . The analysis focuses on key findings like the warning in November from the FBI, CISA and Cyware about a ransomware group that has undergone a stealthy process of metamorphosis otherwise known as **rebranding**. Experts say the **Royal Ransomware** rebranding to **BlackSuit** marks a strategic shift in their operations. This change is not just in name but also reflects in their modus operandi, which includes advanced encryption methods and sophisticated attack vectors.”” Plus, the **cyber mercenaries** who operate within the dark side of some of the most sophisticated spyware on the planet. The highly skilled cyberoperators who learn the craft during their military service in one of the country’s elite signals intelligence units—Unit 8200. “”

Introduction

To this day some of us would rather consider handling a Puffer fish barehanded--knowing there is a 98% chance that you will be injected with the deadly toxin “TTX.” Simply because the thought of hearing your voice exclaim, “I don’t understand X, can you help me.” makes you cringe. Keep reading, I have a survey

Below is a simple painless solution to get you started. Take a moment and check-out the two CISA links below that will help develop:

- **Joint Cyber Defense Collaborative** - Strong strategic and operational alliances within the cybersecurity community.
- **Information Sharing** is the key to preventing a wide-spread cyber-attack. CISA develops partnerships to rapidly share critical information about cyber incidents.

Survey

Help me understand a simple question, by selecting from the list below. 😊

Q: Think of a time when you were faced with a problem you didn't understand but did not want anyone know you couldn't figure out the answer.

What prevented you from asking for help?"

- Fear of Judgment
- Self-Image and Ego
- Cultural and Gender Norms
- Perfectionism
- Lack of Trust
- Fear of Burdening Others
- Communication Skills

Scope

The concept known as—rebranding has been around for a long time. In fact, in 2007, Apple Inc., decided, in order to reflect its expanding product line beyond computers and into a broader range of consumer electronics, like the iPod, iPhone, and iPad. As reported by Cyware Social, the FBI and CISA warn that, "The cybersecurity landscape is continuously evolving, with threat actors often changing tactics and branding to evade detection and expand their operations." The same concept provides cyber bad actors a unique opportunity for a covert metamorphosis or change. ""

We look at a dystopian element of software--cyber mercenaries. On August 31, 2018, Foreign Policy, published, "The Rise of the Cyber-Mercenaries," authored by Neri Zilber, who covers Middle East politics. The article details the sophisticated use of cyber-mercenary technologies by private firms, exemplified by the Israeli NSO Group.
Cyberwar has not only blurred the lines between offense and defense; it has also blurred the notion of sovereign property when it comes to technological development—namely what, exactly, constitutes an Israeli (or U.S. or Chinese) company. The internet has eclipsed borders, and cyberwarfare is no exception. ""

ARTICLE SUMMARY / KEY POINTS

BLASTPASS NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild, TheCitizenLab, 07SEPT2023

Summary

Cozy Bear, a threat group linked with the Russian foreign intelligence service (SVR), has been conducting a global hacking campaign targeting servers hosting JetBrains TeamCity software, according to US, UK and Polish government agencies.
In a joint advisory published on December 13, 2023, six security and intelligence agencies in the US, the UK and Poland warned that Cozy Bear has been exploiting an authentication bypass vulnerability in TeamCity (CVE-2023-42793) since at least September 2023.

Who are Behind the Cozy Bear Moniker?

- Cozy Bear, also known as the Dukes, Nobelium, Midnight Blizzard and APT 29, is a group of highly skilled hackers with reported ties to the Russian foreign intelligence service (SVR).

- Their activity has previously been attributed to the 2016 info-stealing raid on the Democratic National Committee (DNC), the SolarWinds campaign and separate raids targeting intellectual property related to COVID-19 vaccine development.

Key Findings

- **CVE-2023-42897 -** This issue is fixed in iOS 17.2 and iPadOS 17.2. An **attacker** with **physical access** may be able to use Siri to **access sensitive** user **data**. “”
- **Affected Software Versions**: iOS 16.6.1 and iPadOS 16.6.1 “”

Recommendations

- ❖ Given the seriousness of this vulnerability and the **potential for exploitation**, it is strongly recommended that users and administrators promptly update their affected Apple devices to the corresponding fixed software versions mentioned above. Additionally, users should exercise caution when handling image files from untrusted or unknown sources to minimize the risk of exploitation. “”

The Rise of the Cyber-Mercenaries, Foreign Policy, What happens when private firms have cyberweapons as powerful as those owned by government, By Neri Zilber. 31AUG2018.

Summary

Stuxnet is name-checked repeatedly by experts in the field and with good reason: It was a highly successful cyberattack against a state actor that caused real physical damage. Yet Stuxnet may already be outdated as an analytical touchstone. Israel is a world leader in private cybertechnology, with at least 300 firms covering everything from banking security to critical infrastructure defense.

Key Findings

- The Stuxnet virus code is now publicly available. In 2013, a cyberweapon developed by the NSA that exploited vulnerabilities in Microsoft Windows was stolen by hackers—possibly Russian—and posted online; in May 2017, other hackers—possibly North Korean—then used the tool to launch a worldwide ransomware attack. The attack, called WannaCry, is believed to have infected 200,000 computers in more than 150 countries, including major parts of the British National Health Service, before it was rolled back. In a separate 2013 case, Mandiant, a private U.S. cybersecurity firm, proved that hackers affiliated with the Chinese military were targeting U.S. corporations and government agencies. And in 2015, Unit 8200 reportedly hacked into Kaspersky Lab, a global leader in anti-virus software, and discovered that the private company had been acting as a back door for Russian intelligence into its clients, including two dozen U.S. government agencies. “”

- While the international nature of computer technology confers many benefits, it also makes it hard to ascertain the origin of a cyberattack. That lack of attribution then makes it harder for governments to respond, and the lack of a threat of reprisal makes deterrence difficult, if not impossible. “”

Recommendations

- The article "The Rise of the Cyber-Mercenaries" details the sophisticated use of cyber-mercenary technologies by private firms, exemplified by the Israeli NSO Group. that indicative of the blurring lines between defense and offense in cyberspace. Israel's private cybertechnology sector is notable, with firms often staffed by military veterans. The article also discusses broader implications of private cyber capabilities, such as challenges in regulation, the privatization of cyberwarfare tools, and the ethical complexities surrounding the sale and use of such technologies.

Royal Ransomware Rebrands as BlackSuit - Warn FBI and CISA, by Cyware Alerts – Hacker News, Cyware Social , 14NOV2023.

Summary

The cybersecurity landscape is continuously evolving, with threat actors often changing tactics and branding to evade detection and expand their operations. A recent development in this arena involves the Royal ransomware gang. According to a joint advisory from the CISA and the FBI, this group has rebranded itself to BlackSuit.

Key Findings

The rebranding of cybercriminal groups indicates a broader trend in the cybercriminal world, where groups continuously evolve to avoid detection and countermeasures by law enforcement and cybersecurity experts.

- Experts say the rebranding to BlackSuit marks a strategic shift in their operations. This change is not just in name but also reflects in their modus operandi, which includes advanced encryption methods and sophisticated attack vectors.
- In June 2023, Royal ransomware added the BlackSuit encryptor to its tools. This gave rise to suspicions of its preparing for the rebrand.
- Complexities in Attribution: Cybersecurity researchers and government offensive organizations often rely on patterns and historical data to attribute attacks to specific groups. Rebranding can muddy these waters, making it more challenging to attribute new attacks to known groups.
- Diverting Attention from State Sponsorship: In cases where there are allegations of state sponsorship, rebranding can be a tactic to create distance between the cyber group and the sponsoring state. This is particularly relevant in international politics and cyber warfare, where plausible deniability can be crucial. “”

Recommendations

- The **transformation** of the Royal ransomware into BlackSuit is a significant development in the cybersecurity world. It highlights the ever-changing tactics of cybercriminals and the need for constant vigilance. **To mitigate such threats**, organizations must regularly update their security protocols, conduct frequent vulnerability assessments, and invest in employee training to recognize potential cyber threats. “”

- **State-Sponsored vs. State-Tolerated** Activities: There's a distinction between groups directly controlled or sponsored by a state and those that are state-tolerated. In some cases, governments such as China, Iran and Russia tend to turn a blind eye to criminal hackers operating within their jurisdiction, especially if their activities align with national interests or foreign policy objectives. This tacit approval or tolerance can be as significant as direct sponsorship. “”

Terrifying hacks on critical infrastructure have arrived. America isn't ready.
Original article, by Gordon C. Chang, The Hill, 12DEC2023.

Summary

On Nov. 25, an Iran-linked hacker group — with ties to the Iranian state itself — took control of a part of the Municipal Water Authority of Aliquippa, in western Pennsylvania near Pittsburgh. Crews switched to manual systems to deliver water to two towns. The hackers entered the system through Israeli-made programmable logic controller , which had been successfully targeted in attacks in Israel in the past couple of months. The Iranian hackers were able to get in with little effort. Critical infrastructure in the U.S. contains industrial control systems that are known to be easy targets for cyber attackers. “”

Key Findings

- The Iranian hackers were able to get in with little effort. Critical infrastructure in the U.S. contains industrial control systems that are known to be easy targets for cyber attackers.
- Chinese hackers have had their way with American infrastructure networks, reportedly hitting water utilities, major ports and an oil and gas pipeline, to name a few.
- Most analysts are skeptical that Beijing was responsible for the blackouts. Still, in June, Easterly called Chinese cyber-espionage and sabotage an “epoch-defining threat.” Moreover, the 2003 Annual Threat Assessment of the U.S. Intelligence Community states “China almost certainly is capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems.
- Many of these vital networks are, incredibly, permitted to determine on their own what level of security is appropriate, which means they are essentially unprotected. The Aliquippa attack occurred less than a month after the Environmental Protection Agency rescinded a rule requiring water systems to include cybersecurity testing. “”

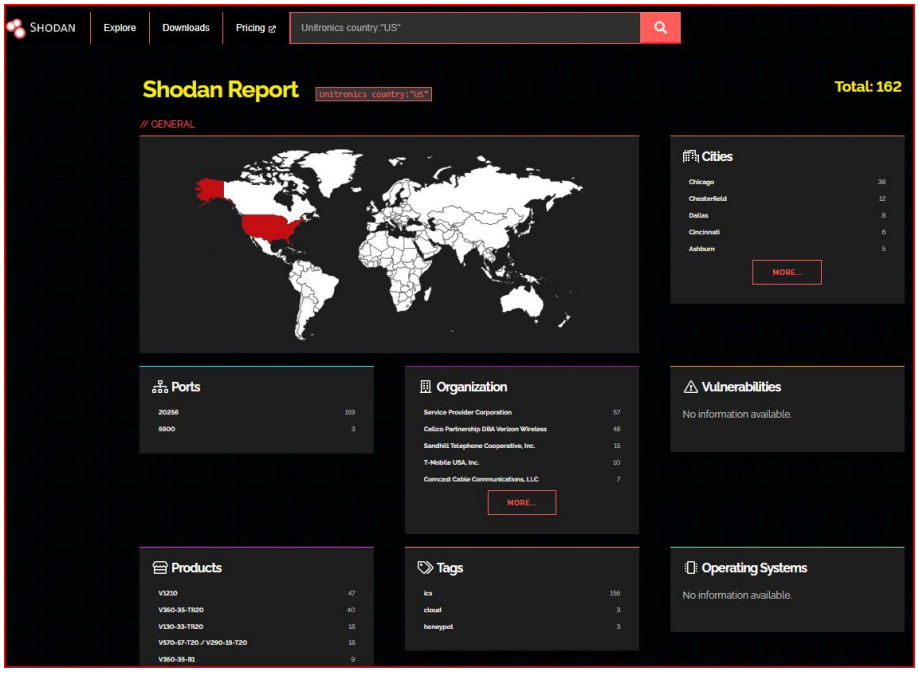
Recommendations

- **CISA** develops partnerships to rapidly share critical information about cyber incidents. **Information sharing** is the **key** to **preventing** a wide-spread **cyber-attack**.

Overview

Information sharing is essential to furthering cybersecurity for the nation. Isolating cyber-attacks and preventing them in the future requires the coordination of many groups and organizations. **By rapidly sharing critical information about attacks and vulnerabilities, the scope and magnitude of cyber events can be greatly decreased**. With the right plans, processes, and connections in place, information sharing can be seamless step of incident response procedures and a first defense against wide-spread cyber-attacks. “”

Shodan Report: Unitronics query result: 1,349 (Global), 162 (US), PLCs identified. ~149 as of 17 DEC. “”



Shodan: On-Demand Scanning

When a server or company resource appears in a Shodan query result, it reflects several key points:

Internet-Facing Presence: The server or resource is connected to the internet. Shodan scans and indexes devices that are accessible over the internet, so appearing in its results indicates that the server or resource is publicly reachable.

IRGC-Affiliated Cyber Actors Exploit PLCs

The IRGC is an Iranian military organization that the United States designated as a foreign terrorist organization in 2019. IRGC-affiliated cyber actors using the persona “**CyberAv3ngers**” are actively targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs). These PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and are additionally used in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare. The PLCs may be rebranded and appear as different manufacturers and companies. In addition to the recent CISA Alert, the authoring agencies are releasing this joint CSA to share indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with IRGC cyber operations. “”

COMPLAINT SECTION

How are we doing? Please send feedback about this newsletter to Fred Ellison.

- E-mail – frederick.s.ellison@uscg.mil

This **electronic** publication is intended to inform port stakeholders about cyber security issues and provide information useful to safeguard seaport systems that may be vulnerable to cyber-attacks. The information contained herein is suitable for general release and members of the Northern California Area Maritime Security Committee are encouraged to pass it on to members of our maritime community. This newsletter will be e-mailed to members of the Northern California Area Maritime Security Committee and posted on the Coast Guard's HOMEPORT portal within the Sector San Francisco port area.

HOW YOU CAN HELP PROTECT CALIFORNIA

State, local, and tribal governments, non-governmental organizations and the private sector can partner with the Cal-CSIC by registering to receive Alerts and Advisories, sharing IOCs and cyber incident reports, and connecting to the California Automated Indicator Exchange.

- Email the Cal-CSIC to learn more about sharing of IOCs and connecting to the California Automated Indicator Exchange at calcsic@caloes.ca.gov.
- Report cyber incidents to the Cal-CSIC at (833) REPORT-1 or calcsic@caloes.ca.gov.

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities, or vessels required to have a Marine Transportation Security Act (MTSA) security plan must report suspicious activities or breaches of security to the Coast Guard's National Response Center (NRC), or **cyber-attacks** to the National Cybersecurity and Communications Integration Center (NCCIC):

- (NRC) Phone 1-800-424-8802 or direct phone line at 202-372-2428
- (NRC) Fax 202-372-2920
- (NRC) Web: http://www.nrc.uscg.mil/
- (NCCIC) at 888-282-0870

After calling the NRC/NCCIC, call the Captain of the Port, San Francisco, at 415-399-3530.

Commented [FE1]: Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan must report suspicious activities or breaches of security to the Coast Guard's National Response Center (NRC), or **cyber-attacks** to the National Cybersecurity and Communications Integration Center (NCCIC):

Other agencies you may want to consider reporting to are:

California Cybersecurity Integration Center – (916) 636-2997 and CalCSIC@caloes.ca.gov

The Federal Bureau of Investigation (FBI) should be notified of cyber security breaches:

- FBI Headquarters – threats and crime reporting: https://tips.fbi.gov/
- San Francisco Office – 415-553-7400 (san.francisco@ic.fbi.gov)
- Sacramento Office – 916-841-9110 (http://www.fbi.gov/sacramento)
- Internet Crime Center – http://www.ic3.gov/complaint/default.aspx
- InfraGard Website – https://www.infragard.org/

U.S. COAST GUARD HOMEPORT PORTAL

The U.S. Coast Guard maintains links to various sources of maritime security information on its HOMEPORT information portal. The link to U.S. Coast Guard's HOMEPORT maritime security information portal is:

- Web – http://www.homeport.uscg.mil/

IF YOU SEE SOMETHING, SAY SOMETHING

To report a crime in progress, call 911 or your local police department. To report maritime related suspicious activities or breaches of security call the National Response Center (NRC) at 800-424-8802 or if a **cyber-attack** to the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870. After calling the NRC or NCCIC call the Captain of the Port, San Francisco, at 415-399-3530.

Note: articles appearing in this newsletter were submitted by port stakeholders or downloaded from public websites and posted without editing. If you have an article to post, please provide the article to Mr. Martin at the above e-mail address. This newsletter is a quarterly publication and generally published shortly before a meeting of the Northern California Area Maritime Security Committee. **This newsletter is for public information purposes only**; articles containing proprietary, sensitive but unclassified, or classified information will not be accepted. The U.S. Coast Guard reserves the right to decide which articles are published in this newsletter.